

Amendments to the Claims:

Please cancel claims 8 and 9 without prejudice. This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) An asymmetric cryptographic processing system using a multiple key hierarchy, the asymmetric cryptographic processing system ~~comprising~~ comprising:
a first key for performing asymmetric operations at a first rate, wherein each operation requires a first cryptographic ~~processing~~ processing time; and
a second key for performing an asymmetric cryptographic processing operation to update the first key, wherein the second key is used in cryptographic processing operations for the first key at a second rate that is less often than the first rate and that ~~require~~ requires a second cryptographic processing time greater than the first cryptographic processing time.
2. (Original) The asymmetric cryptographic processing system of claim 1, wherein the system is used to cryptographically process and transfer digital voice data in a network.
3. (Original) The asymmetric cryptographic processing system of claim 1, wherein the system is used to cryptographically process and transfer digital audio data in a network.
4. (Original) The asymmetric cryptographic processing system of claim 1, wherein the system is used to cryptographically process and transfer digital video data in a network.

5. (Original) The asymmetric cryptographic processing system of claim 1, wherein the system is used to cryptographically process and transfer digital data in a network.

6. (Original) The asymmetric cryptographic processing system of claim 2, wherein the second key is hard coded into the system at the time of manufacturing the system.

7. (Original) The asymmetric cryptographic processing system of claim 6, wherein a plurality of digital cryptographic processing systems are coupled by a telecommunications system, wherein the second key is distributed to two or more of the asymmetric cryptographic processing systems via the telecommunications system.

8. (Canceled)

9. (Canceled)

10. (Currently Amended) A method for providing secure data transactions in a telecommunications system, wherein digital processing device receives information from the telecommunications system, wherein the digital processing device uses a first asymmetrical cryptographically processed key to perform an asymmetric cryptographic processing operation to decode the information, wherein the cryptographic processing operation is at a first level of complexity requiring a first amount of resources by the processing device, wherein the cryptographic processing operation is performed at a first rate of cryptographic processing operations per unit time, the method ~~comprising~~ comprising:

transferring a second asymmetrical cryptographically processed key to the digital processing device, wherein the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources;

updating the first asymmetrical cryptographically processed key from time-to-time, wherein the updating of the first asymmetrical cryptographically processed key occurs at a second rate of cryptographic processing operations per unit time that is less than the

first rate of cryptographic processing operations per unit time, wherein the updating includes the following substeps;

encoding a substitute first asymmetrical cryptographically processed key with a second key, so that the resulting cryptographically processed substitute first asymmetrical cryptographically processed key is decodable by the second asymmetrical cryptographically processed key; and

transferring the substitute first asymmetrical cryptographically processed key to the digital processing device so that the substitute first asymmetrical cryptographically processed key is used in subsequent cryptographic processing operations by the digital processing device.

11. (Currently Amended) The method of claim 7, further ~~comprising~~
comprising:

transferring a third asymmetrical cryptographically processed key to the digital processing device, wherein the third asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a third level of complexity requiring a third amount of resources by the processing device that is higher than the second amount of resources;

updating the second asymmetrical cryptographically processed key from time-to-time, wherein the updating of the second asymmetrical cryptographically processed key occurs at a third rate of cryptographic processing operations per unit time that is less than the second rate of cryptographic processing operations per unit time, wherein the updating includes the following substeps;

encoding a substitute second asymmetrical cryptographically processed key with a third asymmetrical cryptographically processed key, so that the resulting cryptographically processed substitute second asymmetrical cryptographically processed key is capable of being cryptographically processed by the third asymmetrical cryptographically processed key; and

transferring the substitute second asymmetrical cryptographically processed key to the digital processing device so that the substitute second asymmetrical cryptographically processed key is used in subsequent cryptographic processing operations by the digital processing device.

12. (Original) The method of claim 10, wherein the resources include processing time.

13. (Original) The method of claim 10, wherein the resources include transistor density on an integrated circuit.

14. (Original) The method of claim 10, wherein the resources include memory capacity.

15. (Original) The method of claim 10, wherein the resources include data bandwidth.

Please add the following new claims:

16. (New) A method of updating a cryptographic key used for decrypting distributed data, the method comprising:

generating a first key for decrypting the distributed data, the first key of a first length;

encrypting the first key with a second key, the second key of a second length, wherein the second length is longer than the first length; and

distributing the encrypted first key.

17. (New) The method of claim 16, further comprising distributing data encrypted with the first key.

18. (New) The method of claim 17, further comprising:

generating a third key to replace the first key, the third key of a third length, wherein the third length is shorter than the second length;

encrypting the third key with the second key; and

distributing the encrypted third key.

Appl. No. 10/049,812

PATENT

Amdt. dated: November 23, 2005

Reply to Office Action of August 26, 2005

19. (New) The method of claim 18, further comprising distributing data encrypted with the third key.